

SYSTEM AND METHOD FOR ENCRYPTING SPREAD SPECTRUM CARRIER

FEDERAL RESEARCH STATEMENT

[0001] The U.S. Government has a paid-up license in this invention and the right in limited circumstances to require the patent owner to license others on reasonable terms as provided by the terms of Contract No. MDA904-99-9-0001 awarded by the National Security Agency (NSA).

I. Field of the Invention

[0002] The present invention relates generally to the encryption of wireless communication, particularly as regards to spread spectrum communication such as but not limited CDMA and CDMA-type communications.

II. Background of the Invention

[0003] Wireless terminals, such as but not limited to wireless telephones that communicate using Code Division Multiple Access (CDMA) spread spectrum modulation techniques, communicate over the air with system infrastructure using wireless over-the-air communication protocols, e.g., the CDMA protocols known as IS-95A, IS-95B, IS-2000, TD-SCDMA, Large Area Synchronous (LAS-CDMA), and W-CDMA. The system infrastructure, which can include base stations (BTS), base station controllers (BSC), and other components, connects the wireless terminal to another communication device, such as a land line or another wireless communication system.

[0004] To provide for secure communication using spread spectrum wireless systems, encryption principles can be used. For example, U.S. Patent No. 5,727,064 discloses a method for secure communication that encrypts frames of communication (the data symbols, or payload) using a nonlinear scrambler. The scrambler is coupled to the output of the long code generator to remove linearity from the long code sequence produced by the long code generator. Portions of the long code sequence subsequently are combined with the main data signal that is output by the bit interleaver, thereby encrypting frames of data prior to spreading the frames in accordance with spread spectrum communication principles.

[0005] According to the '064 patent, breaking a nonlinear encryption is more difficult to do than breaking an encryption using a linear scrambler. As recognized herein, however, symbol-based encryption, even if nonlinear, remains vulnerable to eavesdropping because it is a relatively small and aligned data payload and is thus less cumbersome to break down and decrypt than a larger and non-aligned payload would be. Moreover, since the frames are encrypted in the above-

mentioned patent, other system control channels, such as the synchronization and pilot channels are not encrypted. With the above considerations in mind, the present invention provides the solutions disclosed below.

SUMMARY OF THE INVENTION

[0006] A method for encrypting spread spectrum wireless communication is disclosed in which the complex-valued scrambling code, e.g., a pseudorandom number (PN) sequence that is used for spreading or scrambling the signal, is encrypted by complex multiplication with data chip sequences. Hence, the present invention essentially encrypts the entire communication, at what amounts to the chip level. As a consequence, the entire communication and not just individual frames or symbols must be broken down and analyzed by an eavesdropper to break the encryption.

[0007] Accordingly, a method for secure wireless communication using spread spectrum principles includes generating at least one pseudorandom number (PN) sequence, and encrypting the PN sequence to render an encrypted PN sequence. Using the encrypted PN sequence, a communication signal is spread and encrypted as a by-product of the spreading operation.

[0008] In a preferred, non-limiting embodiment, the communication signal is received from data modulation circuitry that may include a Walsh modulator. The PN sequence can be encrypted by combining the PN sequence with an encryption sequence (for less preferred BPSK modulation) or two encryption sequences (in the case of QPSK modulation). More encryption sequences as necessary can be used for 8-PSK modulation, QAM-16 modulation, QAM-64 modulation, and so on.

[0009] In a particularly preferred, non-limiting embodiment, the encryption sequence is generated by a DES encryption, such as triple-DES. In this exemplary embodiment, the DES encryption receives input including at least one multi-bit key and at least one time-varying input, such as but not limited to a long code state. If desired, the key periodically can be refreshed.

[0010] In another aspect, a wireless communication system includes a data modulation component that can include a channel coder that codes a communication signal for error correction to produce a coded signal, a bit interleaver for interleaving bits in the coded signal to produce an interleaved coded signal, and a Walsh modulator coupled to the bit interleaver to modulate the interleaved coded signal using a Walsh function. As set forth further below, a carrier modulator spreads the signal from the data modulation component with a pseudorandom number (PN) sequence that is encrypted with at least one encryption sequence.

- [0011] In yet another aspect, a computer program product includes means for encrypting a PN sequence, and means for providing the PN sequence to a spread spectrum communication device for use thereof in spreading or despreading a communication signal.
- [0012] In still another aspect, a chip for use in a communication device includes a data modulation component to produce a Walsh-modulated interleaved coded signal. A carrier modulator spreads the Walsh-modulated interleaved coded signal with a pseudorandom number (PN) sequence that is encrypted with at least one encryption sequence.
- [0013] In another aspect, a chip for use in a communication device includes a PN sequence generator receiving at least one encryption sequence. The PN sequence is combined with the encryption sequence and sent to a despreding component to despread a received spread spectrum communication signal using the combined sequence to render a despread signal. Additional components demodulate, deinterleave, and decode the signal.
- [0014] In another aspect, a method for secure wireless communication using spread spectrum principles includes receiving at least one encryption sequence, and using the encryption sequence to render an encrypted PN sequence. The method also includes using the encrypted PN sequence to despread a received spread spectrum signal to render a despread signal.
- [0015] The details of the present invention, both as to its structure and operation, can best be understood in reference to the accompanying drawings, in which like reference numerals refer to like parts, and in which:

BRIEF DESCRIPTION OF THE DRAWINGS

- [0016] Figure 1 is a block diagram of a presently preferred inventive wireless communication system;
- [0017] Figures 2A and 2B are block diagrams of the transmitting and receiving components, respectively, of a mobile station (MS) and/or the components of a base station (BTS) or other infrastructure component;
- [0018] Figure 3 is a block diagram of one preferred, non-limiting encryption sequence generator;
- [0019] Figure 4 is a schematic block diagram of a conventional mobile station that accesses a software layer to execute the present logic; and
- [0020] Figure 5 is flow chart of the present encryption logic.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0021] Referring initially to Figure 1, a system is shown, generally designated 10, for effecting communication between a wireless communication device 12, referred to herein as a "mobile station," and a telephony infrastructure 14 that includes, e.g., base stations (BTS) 16 (only one BTS 16 shown for clarity), base station controllers (BSC) 18, and additional infrastructure 20 in accordance with wireless communication principles known in the art.

[0022] In accordance with the present invention, the system 10 uses spread spectrum techniques. Accordingly, the mobile station 12 can use an over the air (OTA) protocol such as CDMA or WCDMA to communicate with the infrastructure 14. In one non-limiting embodiment the mobile station 12 is a mobile telephone made by Kyocera, Samsung, or other manufacturer that uses Code Division Multiple Access (CDMA) principles and CDMA over-the-air (OTA) communication air interface and includes protocols such as defined in but not limited to IS-95A, IS-95B, WCDMA, cdma-2000, 1X, IXEV-DO, EV-DV, TD-SDMA, LAS-CDMA, and others to communicate with the infrastructure 14. As is known in the art, IS-95A and IS-95B are examples of spread spectrum protocols that use BPSK data modulation, whereas WCDMA, as an example, is a spread spectrum protocols that uses QPSK data modulation, i.e., split data streams with "I" and "Q" branches.

[0023] For instance, the wireless communication systems to which the present invention can apply, in amplification to those noted above, include Personal Communications Service (PCS) and the following digital systems: CDMA, WCDMA, and hybrid Time Division Multiple Access (TDMA)/CDMA technologies. A CDMA cellular system is described in the Telecommunications Industry Association/Electronic Industries Association (TIA/EIA) Standard IS-95. Other communications systems are described in the International Mobile Telecommunications System 2000/Universal Mobile Telecommunications Systems (IMT-2000/UM), standards covering what are referred to as wideband CDMA (WCDMA), cdma2000 (such as, cdma2000 1x or 3x standards, for example), TD-SCDMA, or LAS-CDMA.

[0024] The present invention applies to any spread spectrum mobile station 12; for illustration it will be assumed that the mobile station 12 is a telephone. In general, wireless communication devices to which the present invention applies may include but are not limited to a wireless handset or telephone, a cellular phone, a data transceiver, or a paging and position determination receiver, and can be hand-held, or portable as in vehicle-mounted (including cars, trucks, boats, planes, trains), as desired. However, while wireless communication devices are generally viewed as being mobile, it is to be understood that the present invention can be applied to "fixed" units in

some implementations. Also, the present invention applies to data modules or modems used to transfer voice and/or data information including digitized video information, and may communicate with other devices using wired or wireless links. Further, the present invention applies to wireless, peer-to-peer communications. Moreover, commands might be used to cause modems or modules to work in a predetermined coordinated or associated manner to transfer information over multiple communication channels simultaneously. Wireless communication devices are also sometimes referred to as user terminals, mobile stations, mobile units, subscriber units, mobile radios or radiotelephones, wireless units, or simply as "users" and "mobiles" in some communication systems.

[0025] Now referring to Figures 2A and 2B, the components of the MS 12 and/or BTS 16 can be seen. That is, either one or both of the MS 12 and BTS 16 can use the present encryption invention in transmission, i.e., either one or both of the uplink (transmissions from the MS 12) or downlink (transmissions from the BTS 16 to the MS 12) can be encrypted with the same or different encrypted PN sequences. It should be noted that to further enhance security, frequency hopping may be employed. Also, not just the traffic channel, but other wireless channels such as pilot channels, synchronization or paging channels or access channels, can be encrypted. It is to be further understood that the BTS 16 can be combined in some systems with the BSC 18, or indeed in mobile switching center (MSC), gateway to a satellite system, or other infrastructure 14 component. Some or all of the components shown in Figure 2 can be embodied in a chip, generally designated 21, or in software as more fully disclosed below in relation to Figures 4 and 5.

[0026] As shown, the chip 21 can include a data modulation component 22 that can include one or more of the following. The component 22 can include a voice coder when the chip 21 is incorporated in a mobile station for encrypting an uplink. The voice coder functions in accordance with wireless communication principles known in the art to generate a data stream representative of a speaker's voice.

[0027] The data modulation component 22 can also include a channel coder that receives the data from the voice coder or other component and codes the signal for error correction in accordance with wireless communication principles known in the art. The coded signal is sent to a bit interleaver of the data modulation component 22 which rearranges the order of the bits to reduce the effect of burst errors. From the bit interleaver, the signal can be sent to a Walsh modulator (or spreader) which Walsh-modulates the signal in accordance with wireless communication principles known in the art by multiplying the signal with a Walsh function.

[0028] The Walsh-modulated signal is then sent to a carrier spreader, e.g., a quadrature carrier spreader or binary carrier spreader 30 which spreads the signal in accordance with spread spectrum communication principles known in the art using a PN sequence. Specifically, the spreader 30 uses an encrypted PN spreading sequence from a PN sequence generator 32 to spread and encrypt the signal. As discussed further below, the PN sequence generator 32 receives from an encryption sequence generator 34 an encryption sequence (when BPSK principles are used), or two encryption sequences (when QPSK principles are used), or as appropriate more than two sequences for 8 bit, 16 bit, and QAM systems. As discussed further below, the encryption sequence generator 34 receives keys.

[0029] Once spread and encrypted, the signal is sent to an impulse modulator 36 that receives a carrier signal to modulate the signal for transmission. The signal can be shaped by a wave shaper if desired and then sent to a transmitter for transmission using an antenna 42.

[0030] In addition to the above-described transmitter portion, the chip 21 can also include a receiver portion, if desired. That is, if desired both the uplink and downlink can be encrypted, or only one side of the communication channel need be encrypted. For completeness, Figure 2 shows a chip 21 that is configured with both a transmitter portion and receiver portion for two-way encryption.

[0031] Accordingly, a receiver antenna 44 is coupled to a processing/amplification component if desired in accordance with principles known in the art, and then the amplified signal is sent to an impulse demodulator 48 which receives a carrier signal for demodulation. The signal is then sent to a despreader 50 that can receive an encrypted PN sequence from the PN sequence generator 32 to despread the signal. It is to be understood that the encrypted PN sequence hypothesis for searching requires an a priori knowledge of estimated time from, e.g., GPS or other source of time information.

[0032] The signal is then processed by a data demodulation component 52 which can include a Walsh demodulator, a bit deinterleaver, and a channel decoder for respectively Walsh demodulating (or despreading) the signal, de-interleaving it, and decoding it in accordance with principles known in the art. When incorporated in a MS, the signal can be sent to a voice decoder to be transformed into an audible signal.

[0033] Having set forth the overall structure of one preferred, non-limiting chip 21, attention is now directed to Figure 3, which shows an exemplary encryption sequence generator. It is to be understood that while Figure 3 shows a circuit useful for QPSK encryption and, thus, shows two

data streams and two encryption sequences, the principles of the present invention apply equally to BPSK (single stream) principles, as well as 8-PSK, 16-QAM, 64-QAM, and other schemes.

[0034] As shown, the spreader 30 can receive first and second data streams D_I and D_Q to produce respective first and second spread data streams using first and second encrypted PN sequences from the PN sequence generator 32. If desired, a HPSK component 53 can be interposed between the spreader 30 and PN sequence generator 32 to reduce peak to average performance. The first and second PN sequences are encrypted by combining a PN sequence with first and second encryption sequences from the encryption sequence generator 34. In one non-limiting, exemplary embodiment, the combination is effected by an XOR operation, although other methods for combining the PN sequence with an encryption sequence can be used.

[0035] A presently preferred, non-limiting encryption sequence generator 34 is illustrated in Figure 3 as having a triple-DES component 60 which outputs first and second serial encryption sequences I_I , I_Q based on one or more parallel bit inputs in accordance with triple-DES principles known in the art. Encryption components other than triple-DES, however, can be used.

[0036] In one illustrative, non-limiting embodiment, the inputs to the triple-DES can be any combination of select portions of a time varying input, such as but not limited to a long code state 62 with companion bits 64 if necessary, or any function thereof. Two sets of inputs such as but not limited to companion bits can be used to respectively establish the first and second encryption sequences I_I , I_Q . Multiple sets of inputs can be used to establish the encryption sequences for a forward link I_I , forward link I_Q , reverse link I_I , and reverse link I_Q .

[0037] Also, secret keys 66 can be input to the triple-DES. These keys 66 can be periodically changed, i.e., refreshed, by means known in the art without service disruption, so that even if the keys 66 are decrypted by an eavesdropper (which would take considerable time, given the chip-level encryption of the present invention), by the time they are decrypted new keys 66 will have been issued, rendering the old keys worthless for further decryption by the eavesdropper. Sixty four, 128, or fewer or more parallel bits can be used as the input to the block ciphers.

[0038] In the case of decryption, the PN sequence of the PN sequence generator 32 is combined with the encryption sequences I_I , I_Q and then used to despread the received data signal.

[0039] Figure 4 shows that alternatively to a chip 21, a conventional spread spectrum MS 70 might access a software layer 72 embodying the present invention. With the above overview of the present architecture in mind, it is to be understood that the present logic is executed on the architecture shown in Figure 4 in accordance with the flow chart of Figure 5. The flow charts herein illustrate the structure of the logic of the present invention as embodied in computer

program software. Those skilled in the art will appreciate that the flow charts illustrate the structures of logic elements, such as computer program code elements or electronic logic circuits, that function according to this invention. Manifestly, the invention is practiced in its essential embodiment by a machine component that renders the logic elements in a form that instructs a digital processing apparatus (that is, a computer, controller, processor, etc.) to perform a sequence of function steps corresponding to those shown.

{0040} In other words, the logic may be embodied by a computer program that is executed by a processor within, e.g., the MS 70 as a series of computer- or control element-executable instructions. These instructions may reside, for example, in RAM or on a hard drive or optical drive, or the instructions may be stored on magnetic tape, electronic read-only memory, or other appropriate data storage device that can be dynamically changed or updated.

{0041} The logic shown in Figure 5 generates the encryption sequence or sequences at block 74 in accordance with the above-disclosed principles. Moving to block 76, the encryption sequence(s) are combined with the PN sequence generated by a PN sequence generator, and then the data signal is spread at block 78 using the encrypted PN sequence.

{0042} While the particular SYSTEM AND METHOD FOR ENCRYPTING SPREAD SPECTRUM CARRIER as herein shown and described in detail is fully capable of attaining the above-described objects of the invention, it is to be understood that it is the presently preferred embodiment of the present invention and is thus representative of the subject matter which is broadly contemplated by the present invention, that the scope of the present invention fully encompasses other embodiments which may become obvious to those skilled in the art, and that the scope of the present invention is accordingly to be limited by nothing other than the appended claims, in which reference to an element in the singular is not intended to mean "one and only one" unless explicitly so stated, but rather "one or more." All structural and functional equivalents to the elements of the above-described preferred embodiment that are known or later come to be known to those of ordinary skill in the art are expressly incorporated herein by reference and are intended to be encompassed by the present claims. Moreover, it is not necessary for a device or method to address each and every problem sought to be solved by the present invention, for it to be encompassed by the present claims. Furthermore, no element, component, or method step in the present disclosure is intended to be dedicated to the public regardless of whether the element, component, or method step is explicitly recited in the claims. No claim element herein is to be construed under the provisions of 35 U.S.C. §112, sixth

paragraph, unless the element is expressly recited using the phrase “means for” or, in the case of a method claim, the element is recited as a “step” instead of an “act.”

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225